Report of the Judicial Conference Committee on Court Administration and Case Management on Privacy and Public Access to Electronic Case Files

Approved by the Judicial Conference of the United States
September 2001

The Judicial Conference of the United States requested that its Committee on Court Administration and Case Management examine issues related to privacy and public access to electronic case files. The Committee on Court Administration and Case Management formed a special subcommittee for this purpose. This subcommittee, known as the Subcommittee on Privacy and Public Access to Electronic Case Files, consisted of four members of the Committee on Court Administration and Case Management: Judge John W. Lungstrum, District of Kansas, Chair; Judge Samuel Grayson Wilson, Western District of Virginia; Judge Jerry A. Davis, Magistrate Judge, Northern District of Mississippi; and Judge J. Rich Leonard, Bankruptcy Judge, Eastern District of North Carolina, and one member from each of four other Judicial Conference Committees (liaison Committees): Judge Emmet Sullivan, District of Columbia, liaison from the Committee on Criminal Law; Judge James Robertson, District of Columbia, liaison from the Committee on Automation and Technology; Judge Sarah S. Vance, Eastern District of Louisiana, liaison from the Committee on the Administration of the Bankruptcy System; and Gene W. Lafitte, Esq., Liskow and Lewis, New Orleans, Louisiana, liaison from the Committee on the Rules of Practice and Procedure. After a lengthy process described below, the Subcommittee on Privacy and Public Access to Electronic Case Files, drafted a report containing recommendations for a judiciary−wide privacy and access policy.

The four liaison Committees reviewed the report and provided comments on it to the full Committee on Court Administration and Case Management. After carefully considering these comments, as well as comments of its own members, the Committee on Court Administration and Case Management made several changes to the subcommittee report, and adopted the amended report as its own.

Brief History of the Committee's Study of Privacy Issues

The Committee on Court Administration and Case Management, through its Subcommittee on Privacy and Public Access to Electronic Case Files (the Subcommittee) began its study of privacy and security concerns regarding public electronic access to case file information in June 1999. It has held numerous meetings and conference calls and received information from experts and academics in the privacy arena, as well as from court users, including judges, court clerks, and government agencies. As a result, in May 2000, the Subcommittee developed several policy options and alternatives for the creation of a judiciary−wide electronic access privacy policy which were presented to the full Committee on Court Administration and Case Management and the liaison committees at their Summer 2000 meetings. The Subcommittee used the opinions and feedback from these committees to further refine the policy options.

In November 2000, the Subcommittee produced a document entitled "Request for Comment on Privacy and Public Access to Electronic Case Files." This document contains the alternatives the Subcommittee perceived as viable following the committees' feedback. The Subcommittee published this document for public comment from November 13, 2000 through January 26, 2001. A website at www.privacy.uscourts.gov was established to publicize the comment document and to collect the comments. Two hundred forty−two comments were received from a very wide range of interested persons including private citizens, privacy rights groups, journalists, private investigators, attorneys, data re−sellers and representatives of the financial services industry. Those comments, in summary and full text format, are available at that website.

On March 16, 2001, the Subcommittee held a public hearing to gain further insight into the issues surrounding privacy and access. Fifteen individuals who had submitted written comments made oral presentations to and answered the questions of Subcommittee members. Following the hearing, the Subcommittee met, considered the comments received, and reached agreement on the policy recommendations contained in this document.

Background

Federal court case files, unless sealed or otherwise subject to restricted access by statute, federal rule, or Judicial Conference policy, are presumed to be available for public inspection and copying. *See Nixon v. Warner Communications, Inc.*, 435 U.S. 589 (1978) (holding that there is a common law right "to inspect and copy public records and documents, including judicial records and documents"). The tradition of public access to federal court case files is also rooted in constitutional principles. *See Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 575−78 (1980). However, public access rights are not absolute, and courts balance access and privacy interests in making decisions about the public disclosure and dissemination of case files. The authority to protect personal privacy and other legitimate interests in nondisclosure is based, like public access rights, in common law and constitutional principles. *See Nixon*, 435 U.S. at 596 ("[E]very court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes").

The term "case file" (whether electronic or paper) means the collection of documents officially filed by the litigants or the court in the context of litigation, the docket entries that catalog such filings, and transcripts of judicial proceedings. The case file generally does not include several other types of information, including non−filed discovery material, trial exhibits that have not been admitted into evidence, drafts or notes by judges or court staff, and various documents that are sometimes known as "left−side" file material. Sealed material, although part of the case file, is accessible only by court order.

Certain types of cases, categories of information, and specific documents may require special protection from unlimited public access, as further specified in the sections on civil, criminal, bankruptcy and appellate case files below. *See United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989) (noting that technology may affect the balance between access rights and privacy and security interests). To a great extent, these recommendations rely upon counsel and litigants to act to protect the interests of their clients and themselves. This may necessitate an effort by the courts to educate the bar and the public about the fact that documents filed in federal court cases may be available on the Internet.

It is also important to note that the federal courts are not required to provide electronic access to case files (assuming that a paper file is maintained), and these recommendations do not create any entitlement to such access. As a practical matter, during this time of transition when courts are implementing new practices, there may be disparity in access among courts because of varying technology. Nonetheless, the federal courts recognize that the public should share in the benefits of information technology, including more efficient access to court case files.

These recommendations propose privacy policy options which the Committee on Court Administration and Case Management (the Committee) believes can provide solutions to issues of privacy and access as those issues are now presented. To the extent that courts are currently experimenting with procedures which differ from those articulated in this document, those courts should reexamine those procedures in light of the policies outlined herein. The Committee recognizes that technology is ever changing and these recommendations may require frequent re−examination and revision.

Recommendations

The policy recommended for adoption by the Judicial Conference is as follows:

General Principles

- There should be consistent, nationwide policies in federal courts in order to ensure that similar privacy protections and access presumptions apply regardless of which federal court is the custodian of a particular case file.

- Notice of these nationwide policies should be given to all litigants in federal court so that they will be aware of the fact that materials which they submit in a federal court proceeding could become available on the Internet.

- Members of the bar must be educated about the policies and the fact that they must protect their clients by carefully examining the documents that they file in federal court for sensitive, private information and by making the appropriate motions to protect documents from electronic access when necessary.
- Except where otherwise noted, the policies apply to both paper and electronic files.

- Electronic access to docket sheets through PACERNet and court opinions through court websites will not be affected by these policies.

- The availability of case files at the courthouse will not be affected or limited by these policies.
- Nothing in these recommendations is intended to create a private right of action or to limit the application of Rule 11 of the Federal Rules of Civil Procedure.

Case Types

Civil Case Files

Recommendation: That documents in civil case files should be made available electronically to the same extent that they are available at the courthouse with one exception (Social Security cases should be excluded from electronic access) and one change in policy (the requirement that certain "personal data identifiers" be modified or partially redacted by the litigants). These identifiers are Social Security numbers, dates of birth, financial account numbers and names of minor children.

The recommendation provides for liberal remote electronic access to civil case files while also adopting some means to protect individual privacy. Remote electronic access will be available only through the PACERNet system which requires registration with the PACER service center and the use of a log in and password. This creates an electronic trail which can be retraced in order to determine who accessed certain information if a problem arises. Further, this recommendation contemplates that certain personal, identifying information will not be included in its full and complete form in case documents, whether electronic or hard copy. For example, if the Social Security number of an individual must be included in a document, only the last four digits of that number will be used whether that document is to be filed electronically or at the courthouse. If the involvement of a minor child must be mentioned, only that child's initials should be used; if an individual's date of birth is necessary, only the year should be used; and, if financial account numbers are relevant, only the last four digits should be recited in the document. It is anticipated that as courts develop local rules and instructions for the use and implementation of Electronic Case Filing (ECF), such rules and instructions will include direction on the truncation by the litigants of personal identifying information. Similar rule changes would apply to courts which are imaging documents.

Providing remote electronic access equal to courthouse access will require counsel and pro se litigants to protect their interests through a careful review of whether it is essential to their case to file certain documents containing private sensitive information or by the use of motions to seal and for protective orders. It will also depend upon the discretion of judges to protect privacy and security interests as they arise in individual cases. However, it is the experience of the ECF prototype courts and courts which have been imaging documents and making them electronically available that reliance on judicial discretion has not been problematic and has not dramatically increased or altered the amount and nature of motions to seal. It is also the experience of those courts that have been making their case file information available through PACERNet that there have been virtually no reported privacy problems as a result.

This recommended "public is public" policy is simple and can be easily and consistently applied nationwide. The recommended policy will "level the geographic playing field" in civil cases in federal court by allowing attorneys not located in geographic proximity to the courthouse easy access. Having both remote electronic access and courthouse access to the same information will also utilize more fully the technology available to the courts and will allow clerks' offices to better and more easily serve the needs of the bar and the public. In addition, it might also discourage the possible development of a "cottage industry" headed by data re−sellers who, if remote electronic access were restricted, could go to the courthouse, copy the files, download the information to a private website, and charge for access to that website, thus profiting from the sale of public information and undermining restrictions intended to protect privacy.

Each of the other policy options articulated in the document for comment presented its own problems. The idea of defining what documents should be included in the public file was rejected because it would require the courts to restrict access at the courthouse to information that has traditionally been available from courthouse files. This would have the net effect of allowing less overall access in a technological age where greater access is easy to achieve. It would also require making the very difficult determination of what information should be included in the public file.

The Committee seriously considered and debated at length the idea of creating levels of access to electronic documents (i.e., access to certain documents for specific users would be based upon the user's status in the case). The Committee ultimately decided that levels of access restrictions were too complicated in relation to the privacy benefits which could be derived therefrom. It would be difficult, for example, to prohibit a user with full access to all case information, such as a party to the case, from downloading and disseminating the restricted information. Also, the levels of access would only exist in relation to the remote electronic file and not in relation to the courthouse file. This would result in unequal remote and physical access to the same information and could foster a cottage industry of courthouse data collection as described above.

Seeking an amendment to the Federal Rules of Civil Procedure was not recommended for several reasons. First, any such rules amendment would take several years to effectuate, and the Committee concluded that privacy issues need immediate attention. There was some discussion about the need for a provision in Fed. R. Civ. P. 11 providing for sanctions against counsel or litigants who, as a litigation tactic, intentionally include scurrilous or embarrassing, irrelevant information in a document so that this information will be available on the Internet. The Committee ultimately determined that, at least for now, the current language of Fed. R. Civ. P. 11 and the inherent power of the court are sufficient to deter such actions and to enforce any privacy policy.

As noted above, this recommendation treats Social Security cases differently from other civil case files. It would limit remote electronic access. It does contemplate, however, the existence of a skeletal electronic file in Social Security cases which would contain documents such as the complaint, answer and dispositive cross motions or petitions for review as applicable but **not** the administrative record and would be available to the court for statistical and case management purposes. This recommendation would also allow litigants to electronically file documents, except for the administrative record, in Social Security cases and would permit electronic access to these documents by litigants only.

After much debate, the consensus of the Committee was that Social Security cases warrant such treatment because they are of an inherently different nature from other civil cases. They are the continuation of an administrative proceeding, the files of which are confidential until the jurisdiction of the district court is invoked, by an individual to enforce his or her rights under a government program. Further, all Social Security disability claims, which are the majority of Social Security cases filed in district court, contain extremely detailed medical records and other personal information which an applicant must submit in an effort to establish disability. Such medical and personal information is critical to the court and is of little or no legitimate use to anyone not a party to the case. Thus, making such information available on the Internet would be of little public benefit and would present a substantial intrusion into the privacy of the claimant. Social Security files would still be available in their entirety at the courthouse.

Criminal Case Files

Recommendation: That public remote electronic access to documents in criminal cases should not be available at this time, with the understanding that the policy will be reexamined within two years of adoption by the Judicial Conference.

The Committee determined that any benefits of public remote electronic access to criminal files were outweighed by the safety and law enforcement risks such access would create. Routine public remote electronic access to documents in criminal case files would allow defendants and others easy access to information regarding the cooperation and other activities of defendants. Specifically, an individual could access documents filed in conjunction with a motion by the government for downward departure for substantial assistance and learn details of a defendant's involvement in the government's case. Such information could then be very easily used to intimidate, harass and possibly harm victims, defendants and their families.

Likewise, routine public remote electronic access to criminal files may inadvertently increase the risk of unauthorized public access to preindictment information, such as unexecuted arrest and search warrants. The public availability of this information could severely hamper and compromise investigative and law enforcement efforts and pose a significant safety risk to law enforcement officials engaged in their official duties. Sealing documents containing this and other types of sensitive information in criminal cases will not adequately address the problem, since the mere fact that a document is sealed signals probable defendant cooperation and covert law enforcement initiatives.

The benefit to the public of easier access to criminal case file information was not discounted by the Committee and, it should be noted that, opinions and orders, as determined by the court, and criminal docket sheets will still be available through court websites and PACER and PACERNet. However, in view of the concerns described above, the Committee concluded that individual safety and the risk to law enforcement personnel significantly outweigh the need for unfettered public remote access to

the content of criminal case files. This recommendation should be reconsidered if it becomes evident that the benefits of public remote electronic access significantly outweigh the dangers to victims, defendants and their families, and law enforcement personnel.

Bankruptcy Case Files

Recommendation: That documents in bankruptcy case files should be made generally available electronically to the same extent that they are available at the courthouse, with a similar policy change for personal identifiers as in civil cases; that § 107(b)(2) of the Bankruptcy Code should be amended to establish privacy and security concerns as a basis for the sealing of a document; and that the Bankruptcy Code and Rules should be amended as necessary to allow the court to collect a debtor's full Social Security number but display only the last four digits.

The Committee recognized the unique nature of bankruptcy case files and the particularly sensitive nature of the information, largely financial, which is contained in these files; while this recommendation does provide open remote electronic access to this information, it also accommodates the privacy concerns of individuals. This recommendation contemplates that a debtor's personal, identifying information and financial account numbers will not be included in their complete forms on any document, whether electronic or hard copy (i.e., only the last four digits of Social Security and financial account numbers will be used). As the recommendation recognizes, there may be a need to amend the Bankruptcy Code to allow only the last four digits of an individual debtor's Social Security number to be used. The bankruptcy court will collect the full Social Security number of debtors for internal use, as this number appears to provide the best way to identify multiple bankruptcy filings. The recommendation proposes a minor amendment to § 107(a) to allow the court to collect the full number, but only display the last four digits. The names of minor children will not be included in electronic or hard copies of documents.

As with civil cases, the effectiveness of this recommendation relies upon motions to seal filed by litigants and other parties in interest. To accomplish this result, an amendment of 11 U.S.C. § 107(b), which now narrowly circumscribes the ability of the bankruptcy courts to seal documents, will be needed to establish privacy and security concerns as a basis for sealing a document. Once again, the experiences of the ECF prototype and imaging courts do not indicate that this reliance will cause a large influx of motions to seal. In addition, as with all remote electronic access, the information can only be reached through the log−in and password− controlled PACERNet system.

The Committee rejected the other alternatives suggested in the comment document for various reasons. Any attempt to create levels of access in bankruptcy cases would meet with the same problems discussed with respect to the use of levels of access for civil cases. Bankruptcy cases present even more issues with respect to levels of access because there are numerous interests which would have a legitimate need to access file information and specific access levels would need to be established for them. Further, many entities could qualify as a "party in interest" in a bankruptcy filing and would need access to case file information to determine if they in fact have an interest. It would be difficult to create an electronic access system which would allow sufficient access for that determination to be made without giving full access to that entity.

The idea of collecting less information or segregating certain information and restricting access to it was rejected because the Committee determined that there is a need for and a value in allowing the public access to this information. Further, creating two separate files, one totally open to the public and one with restricted access, would place a burden on clerks' offices by requiring the management of two sets of files in each case.

Appellate Case Files

Recommendation: That appellate case files be treated at the appellate level the same way in which they are treated at the lower level.

This recommendation acknowledges the varying treatment of the different case types at the lower level and carries that treatment through to the appellate level. For cases appealed to the district court or the court of appeals from administrative agencies, the documents in the appeal will be treated, for the purposes of remote electronic access, in the same manner in which they were treated by the agency. For cases appealed from the district court, the case file will be treated in the manner in which it was treated by the district court with respect to remote electronic access.